IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JEFFREY SCHWARTZ, Plaintiff, vs. **SUPPLY NETWORK, INC., d/b/a Viking SupplyNet**, a foreign corporation, Defendant.	Case No.: 1:23-cv-14319 **JURY TRIAL DEMANDED**

COMPLAINT

JEFFREY SCHWARTZ ("Plaintiff"), through counsel, for his Complaint against Defendant, SUPPLY NETWORK, INC., d/b/a Viking SupplyNet ("Defendant"), states:

NATURE OF THE CASE

1. This is an action to recover statutory damages and for injunctive relief arising out of Defendant's unlawful collection, receipt, use, and possession of the personal biometric identifiers and biometric information of Plaintiff in violation of the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 (2008).

THE PARTIES

2. Plaintiff is a natural person who is domiciled in Illinois.

3. Defendant is a foreign corporation with its principal place of business in Caledonia, Michigan.

4. Defendant operates a facility known as "Viking SupplyNet" at 640 Center Avenue, Carol Stream, Illinois that distributes the largest selection of fire sprinkler system components across the world.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a) as the matter in controversy exceeds $75,000.00[1] exclusive of punitive damages, and/or interest and costs, and is between citizens of different States.

6. Plaintiff is a citizen of Illinois.

7. Defendant is a citizen of Michigan.

8. This Court has personal jurisdiction over Defendant because it conducts substantial business in Illinois.

9. Venue lies in this District pursuant to 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District and Defendant can be found in this District.

RELEVANT FACTS

10. Plaintiff worked at Defendant's Carol Stream, Illinois facility as a delivery driver.

11. Plaintiff worked at Defendant's facility from October 2017 through June 2022.

12. During the time Plaintiff worked at Defendant's facility, Defendant used a time clock system that required Plaintiff to scan and input his fingerprint or hand geometry to identify him so he could clock in and of work and for breaks.

13. Defendant's time clock system collected, used and stored a scan of Plaintiff's fingerprint or hand geometry for purposes of time tracking and employee authentication.

14. Alternatively, Defendant's time clock system collected, used and stored an encrypted mathematical representation of Plaintiff's fingerprint's or hand geometry's characteristics.

[1]Plaintiff seeks statutory, liquidated damages of $1,000 to $5,000 for each violation of BIPA and alleges that there were not less than 1,000 BIPA violations.

15. In either event, Defendant's time clock system used, collected, and stored unique "biometric identifiers" and "biometric information," as both terms are defined below, belonging to Plaintiff.

16. Defendant did not seek Plaintiff's consent prior to collecting, using or storing his biometric identifiers or information.

17. Defendant was required to destroy Plaintiff's biometric identifiers and information no later than three years after the conclusion of his employment and did not do so.

18. Defendant did not have in place a post-employment biometric retention and destruction policy at any time during Plaintiff's employment.

19. Prior to collecting and/or receiving Plaintiff's biometric identifiers or information, Defendant did not inform Plaintiff in writing that his biometrics were being collected, stored, and used.

20. Plaintiff also did not consent to Defendant disseminating or disclosing any of his biometric identifiers or information that it collected.

21. Plaintiff's biometric identifiers or information were collected, used, stored, disclosed or disseminated in violation of BIPA not less than 1,000 times during the course of his employment at Defendant's Carol Stream facility within the last five years.

HARM TO PLAINTIFF

22. While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed,

employees have no means by which to prevent identity theft and unauthorized tracking. If a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

23. A nefarious market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018).[2]

24. In 2015, a hacking event of the U.S. Office of Personnel Management caused 5.6 million people's fingerprints to compromised. *See* April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016).[3]

25. By 2019, biometrics were expected to become a 25-billion-dollar industry with more than 500 million biometric scanners in use around the world. Chiara A. Sottile, *As Biometric Scanning Use Grows, So Does Security Risk*, NBC NEWS: MACH (July 24, 2016, 6:29 PM).[4]

[2] Available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security -breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259fl38. (last accessed 9/29/2023)

[3] Available at https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns (last accessed 9/29/2023)

[4] Available at https://www.nbcnews.com/mach/mach/biometricscanning-use-grows-so-do-security-risks-ncna593161. (last accessed 9/29/2023)

26. The use of biometric information for timekeeping has become so common in an employment setting as to be almost ubiquitous. Companies use biometric devices as a more secure way to authenticate employee identity for timekeeping, to grant access to sensitive data, or to facilitate onboarding and offboarding. Companies use biometric systems to ensure that workers using a time clock are who they say they are and to avoid "buddy punching." Biometric time clocks that use fingerprint scanning or facial recognition can also help companies better comply with labor laws by ensuring employees clock in and out accurately. *See* Jay Hux, *Collecting Employee Biometric Data Could Prove Costly in Illinois*, SHRM: ST. & LOC. UPDATES (Sept. 19, 2017).

27. On May 18, 2023, the Federal Trade Commission voted 3-0 and adopted a new policy statement on Biometric Information and Section 5 of the Federal Trade Commission Act.[5] The decision to adopt the new policy reflects the FTC's significant concerns about biometric information and related technologies with respect to privacy, security and other issues.

28. In commenting on the above policy statement, Samuel Levine, Director of the FTC's Bureau of Consumer Protection, said: "In recent years, biometric surveillance has grown more sophisticated and pervasive, posing new threats to privacy and civil rights," "Today's policy statement makes clear that companies must comply with the law regardless of the technology they are using."[6]

29. In late 2007, a biometrics company called Pay by Touch - which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions - filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records - which, like other

[5] Available at https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. (last accessed 9/29/2023)

[6] *See* https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers (last accessed 9/29/2023)

unique biometric identifiers, can be linked to people's sensitive financial and personal data - could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

30. Recognizing the need to protect its citizens from situations like these, in 2008, Illinois enacted BIPA in light of the "very serious need [for] protections for the citizens of Illinois when it comes to [their] biometric information."[7]

31. BIPA was enacted with the understanding that "the full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f). The legislature specifically found that persons who have their biometrics taken unlawfully are at increased risk of future injury. *Id.*

32. The legislature recognized that biometrics are unlike other unique identifiers used to access finances or other sensitive information. "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[8]

33. To address this legitimate concern, Section 15(b) of BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

[7] 95th Ill. Gen. Assem. House Proceedings, May 30, 2008, at 249 (statement of Representative Ryg), available at http://www.ilga.gov/house/transcripts/htrans95/09500276.pdf.
[8] 740 ILCS 14/5(c).

> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[9]

34. For BIPA purposes, a "biometric identifier" is a personal feature that is unique to an individual and specifically includes fingerprints.

35. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based upon an individual's biometric identifier used to identify the individual."[10]

36. BIPA specifically applies to employees who work in the State of Illinois.

37. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

38. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and fingerprints. *See* 740 ILCS 14/10.

39. Biometric information is separately defined to include any information based on an identifier that is used to identify an individual. *See id*.

40. BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See* 740 ILCS 14/15(c)-(d). BIPA makes it unlawful for companies to "sell, lease, trade, or otherwise profit from a person's or a customer's

[9] 740 ILCS 14/15(b).
[10] *Id.*

biometric identifier or biometric information." Furthermore, no company may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless":

> (1) the person or customer consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the person or customer;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

See 740 ILCS 14/15(c)-(d).

41. Ultimately, BIPA is an informed consent statute. Its narrowly tailored provisions place no absolute bar on collecting, sending, transmitting or communicating of biometric data. For example, BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does BIPA limit from whom biometric data may be collected, to whom it may be sent, transmitted, or stored. BIPA merely mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

42. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's repeated violations of BIPA alleged herein.

43. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems that it used would be subject to the provisions of BIPA, a law in effect since 2008, yet wholly failed to comply with the statute.

44. Alternatively, Defendant negligently failed to comply with BIPA by failing to adhere to the reasonable standard of care in its industry with respect to employee biometric identifiers or information. 740 ILCS 14/15(e).

45. Plaintiff now seeks statutory, liquidated damages under BIPA as compensation for the Defendant's multiple violations of BIPA.

46. Plaintiff also seeks a declaration that Defendant's actions in contravention of BIPA are unlawful and to enjoin Defendant from further violations of BIPA.

47. This lawsuit constitutes Plaintiff's one and only chance at compensation for Defendant's violations of BIPA. Depending on how technology evolves years into the future, losing control of and ownership over very personal identifiers could have untold harmful consequences.

48. The Illinois legislature concluded that the increased risk of future harm is a compensable loss under the BIPA. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 35, 129 N.E.3d 1197, 1206 citing 740 ILCS 14/5(c) (noting increased risk of identity theft should biometrics be compromised); *Dillon v. Evanston Hosp.*, 199 Ill. 2d 483, 507, 771 N.E.2d 357, 372 (2002) (Illinois Supreme Court finding risk of future injury compensable as an element of damages in medical malpractice case). The legislature's decision is particularly reasonable given that the statute of limitations on BIPA claims presumably runs from the date of the collection of biometrics, whereas the future injury may not occur until after the statute has run.

49. Plaintiff seeks an award of liquidated damages, which is appropriate given that this harm is difficult to quantify.

50. No amount of time or money can compensate Plaintiff if his biometric data is or has been compromised by the lax procedures through which Defendant collects, captures, obtains, stores, disseminates, and/or uses Plaintiff's biometrics.

51. Moreover, Plaintiff would not have provided his biometric data to Defendant if he had known that Defendant would retain such information for an indefinite period of time without their consent.

52. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act"). 65. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40.

COUNT I

Violation of §15(a) of BIPA
[Failure to Institute, Maintain, and Adhere to Publicly Available Retention Schedule]

53. Plaintiff restates paragraphs 1 through 52 of the complaint as if set out here in full.

54. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention - and, importantly, deletion - policy. Specifically, these companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 15(a).

55. Defendant is an entity registered to do business in Illinois and thus it qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

56. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints or hand geometry) collected by Defendant. *See* 740 ILCS 14/10.

57. Plaintiff's biometric identifiers were used to identify him and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

58. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 15(a).

59. Defendant failed to make any written policy establishing a retention schedule and guidelines for permanent deletion of biometric data publicly available.

60. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's biometric data and has not destroyed Plaintiff's biometric data when the purpose for collecting or obtaining such data has been satisfied or within 3 years of the individual's last interaction with the company.

61. Plaintiff has never seen, been able to access, or been informed of any publicly available biometric data retention policy or guidelines developed by Defendant, nor has he ever seen, been able to access, or been informed of whether Defendant would ever permanently delete his biometric data.

62. Defendant knew, or was reckless in not knowing, that the biometric timekeeping system it used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with Section 15 (a) of BIPA, or otherwise intentionally or recklessly failed to comply with Section 15 (a) of BIPA.

63. Alternatively, Defendant negligently failed to comply with Section 15 (a) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15 (a) of BIPA.

64. Plaintiff seeks statutory damages of $5,000 for each willful and/or reckless violation of Section 15(a) BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); and reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II

Violation of §15(b) of BIPA
[Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information]

65. Plaintiff restates paragraphs 1 through 52 of the complaint as if set out here in full.

66. BIPA requires a company to obtain informed written consent from its workers before acquiring their biometric data.

67. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

68. "A party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection." *Cothron v. White Castle System, Inc.*, 2023 IL 128004 ¶ 24 (internal citation omitted).

69. Informed consent is the "heart of BIPA." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020).

70. Defendant is an entity registered to do business in Illinois and thus it qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

71. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints or hand geometry) collected by Defendant. *See* 740 ILCS 14/10.

72. Plaintiff's biometric identifiers were used to identify him and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

73. Defendant collected, captured or otherwise obtained Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

74. Defendant did not inform Plaintiff in writing that his biometric identifier or biometric information was being collected or stored, or of the specific length of term for which his biometric identifiers and/or biometric information were being collected, stored or used before collecting, storing or using them as required by 740 ILCS 14/15(b)(1)-(2).

75. Prior to collecting Plaintiff's biometric identifiers and information, Defendant did not obtain a written release authorizing such collection. 740 ILCS 14/15(b)(3).

76. By collecting, storing, and using Plaintiff's biometric identifiers or information as described herein, Defendant violated Plaintiff's privacy in his biometric identifiers and information as set forth in BIPA *each time* the Defendant collected, captured, obtained, stored or used his biometric identifiers or information. *See* 740 ILCS 14/1, *et seq.*; *Cothron v. White Castle System, Inc.*, 2023 IL 128004 ¶ 24. "[T]he plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission." *Id.* At ¶ 30.

77. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with Section 15 (b) of BIPA, or otherwise intentionally or recklessly failed to comply with Section 15 (b) of BIPA.

78. Alternatively, Defendant negligently failed to comply with Section 15 (b) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15 (b) of BIPA.

79. Plaintiff seeks statutory damages of $5,000 for each willful and/or reckless violation of Section 15(b) BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); and reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT III

Violation of §15(d) of BIPA
[Disclosure of Biometric Identifiers or Information Without Obtaining Consent]

80. Plaintiff restates paragraphs 1 through 52 of the complaint as if set out here in full.

81. BIPA prohibits private entities from disclosing, redisclosing or otherwise disseminating a person's or customer's biometric identifier or biometric information without obtaining consent for that disclosure, redisclosure or dissemination, with limited exceptions, none of which are appliable here. 740 ILCS 14/15(d).

82. Defendant is an entity registered to do business in Illinois and thus it qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

83. Plaintiff is an individual who had his "biometric identifiers" (in the form of his fingerprints or hand geometry) collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

84. Plaintiff's biometric identifiers were used to identify him and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

85. Upon information and belief, by utilizing a biometric time clock, Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated biometric identifiers or biometric information of Plaintiff to at least its payroll vendor without obtaining the Plaintiff's consent required by 740 ILCS 14/15(d)(1).

86. By disclosing, redisclosing, or otherwise disseminating Plaintiff's biometric identifiers and biometric information without his consent as described herein, Defendant violated BIPA *each time* there was a disclosure, redisclosure or dissemination of the Plaintiff's biometric identifiers in violation of Plaintiff's right to privacy in his biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

87. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with the statute, or otherwise intentionally or recklessly failed to comply with Section 15 (b) of BIPA.

88. Alternatively, Defendant negligently failed to comply with Section 15(d) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15(d) of BIPA.

89. "[T]he plain language of section 15(d) supports the conclusion that a claim accrues upon each transmission of a person's biometric identifier or information without prior informed consent." *White Castle System, Inc*., 2023 IL 128004 at ¶ 29.

90. Plaintiff seeks statutory damages of $5,000 for each willful and/or reckless violation of Section 15(d) BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory

damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); and reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court enter judgment in his favor and against Defendant declaring that Defendant's actions, as set forth above, violate BIPA; enjoining Defendant from committing further violations of BIPA; awarding Plaintiff statutory, liquidated damages for each of Defendant's violations of BIPA; and awarding Plaintiff his reasonable litigation expenses and attorneys' fees pursuant to 740 ILCS 14/20.

JURY DEMAND

Plaintiff hereby respectfully demands a trial by jury.

Respectfully submitted,

JEFFREY SCHWARTZ

/s/ Adam J. Feuer

Adam J. Feuer
Majdi Hijazin
DC LAW, PLLC
20 North Clark Street
Suite 3300
Chicago, Illinois 60602
(872) 804-3400
adam@chicagojustice.law
majdi@chicagojustice.law

Nick Wooten
DC LAW, PLLC
1012 West Anderson Lane
Austin, Texas 78757
(512) 220-1800
nick@texasjustice.com
Lead Trial Attorney

Counsel for Plaintiff